UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/809,073	03/16/2001	Lee Codel Lawson Tarbotton	550-221	5551

7590 09/21/2004

NIXON & VANDERHYE P.C.
1100 North Glebe Road, 8th Floor
Arlington, VA 22201-4714

EXAMINER	
SIMITOSKI, MICHAEL J	
ART UNIT	**PAPER NUMBER**
2134	

DATE MAILED: 09/21/2004

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)
	09/809,073	TARBOTTON ET AL.
	Examiner	Art Unit
	Michael J Simitoski	2134

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *16 March 2001*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-42* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-42* is/are rejected.

7)☒ Claim(s) *5,19 and 33* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *16 March 2001* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 1-42 are pending.

Drawings

2. New corrected drawings in compliance with 37 CFR 1.121(d) are required in this application because the drawings are handwritten with text and graphics that are difficult to read. Applicant is advised to employ the services of a competent patent draftsperson outside the Office, as the U.S. Patent and Trademark Office no longer prepares new drawings. The corrected drawings are required in reply to the Office action to avoid abandonment of the application. The requirement for corrected drawings will not be held in abeyance.

Specification

3. The abstract of the disclosure is objected to because "A anti-computer virus" in the first line should be replaced with "An anti-computer virus". Correction is required. See MPEP § 608.01(b).

4. The disclosure is objected to because of the following informalities: the following misspelled words should be corrected:

"organisation(s)" (page 1, ¶3, page 3, ¶1 & page 7, ¶2) should be replaced with "organization(s)",

"utilising"/"utilised" (page 2, ¶5, page 3, ¶3 & page 6, ¶4), should be replaced with "utilizing"/"utilizing",

"characterising" (page 5, ¶5) should be replaced with "characterizing",

"behavioural" (page 6, ¶6) should be replaced with "behavioral", and

"analysed" (page 6, ¶6) should be replaced with "analyzed".

Appropriate correction is required.

Claim Objections

5. Claim 5, 19 & 33 are objected to because of the following informalities: "behavioural" (lines 2 & 4 of each claim) should be replaced with "behavioral". Appropriate correction is required.

Claim Rejections - 35 USC § 112

6. The following is a quotation of the first paragraph of 35 U.S.C. 112:

> The specification shall contain a written description of the invention, and of the manner and process of making and using it, in such full, clear, concise, and exact terms as to enable any person skilled in the art to which it pertains, or with which it is most nearly connected, to make and use the same and shall set forth the best mode contemplated by the inventor of carrying out his invention.

7. Claims 3, 9, 17, 23, 31 & 37 are rejected under 35 U.S.C. 112, first paragraph, as failing to comply with the enablement requirement. The claim(s) contains subject matter which was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. The specification does not describe a "PGP private key" so as to differentiate it from a "private key". *For the purposes of this Office Action, a "PGP private key" is understood to mean a "private key" used in conjunction with the PGP program.*

8. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

9. Claims 3, 9, 17, 23, 31 & 37 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. The claims recite "PGP private key" and "PGP public key" and, as best understood, this refers to public and private keys used with the PGP program; however, as described in "How PGP Works" by Network Associates, the PGP program uses the public/private keys to encrypt secret session keys, rather than data, and therefore the scope of "PGP private key" and "PGP public key" is unclear. *For the purposes of this Office Action, inasmuch as "PGP private key" and "PGP public key" are used in the claimed invention, they are understood to be equivalent to a public and private key pair and encryption/decryption performed with the PGP private/public keys is that of standard public key algorithms.*

Claim Rejections - 35 USC § 103

10. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

11. Claims 1, 4, 6-7, 11-15, 18, 20-21, 25-29, 32, 34-35 & 39-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over "Norton AntiVirus User's Guide", by Symantec Corporation (Symantec) in view of "Combating computer viruses: IBM's new computer immune system" by Hedberg.

Regarding claims 1, 4, 6-7, 14-15, 18, 20-21, 28-29, 32, 34-35 & 42, Symantec discloses a user controlled program identifying data generating logic/Norton AntiVirus to generate banned program identifying data/encrypted suspected virus for said one or more computer programs/suspected viruses to be banned from use/quarantined (page 31, ¶1, page 45, §Submitting files to SARC & page 46). Symantec lacks said banned program identifying data/encrypted suspected virus being operable to control anti computer virus logic to identify computer programs banned from use. However, Hedberg teaches that anti-virus software can be made to detect variations of known viruses and extract identification signatures for them (pages 10-11 & Fig. 1) to eliminate the need for the slower traditional approach (page 10, §A neural network virus classifier). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to create banned program identifying data that is operable to control anti computer virus logic to identify the computer programs/viruses banned from use. One of ordinary skill in the art would have been motivated to perform such a modification to eliminate the need for the slower (page 10, §A neural network virus classifier) traditional analysis approach, as taught by Hedberg (pages 10-11 & Fig. 1).

Regarding claims 11, 25 & 39, Symantec discloses that the program can be encrypted/quarantined or deleted (pages 39-40).

Regarding claims 12, 26 & 40, Symantec, as modified above, discloses restoring the banned program identifying data/virus definitions from a remote source/LiveUpdate server (page 18).

Regarding claims 13, 27 & 41, Symantec, as modified above, lacks explicit disclosure of the anti computer virus logic being executable as a separate instance solely to identify computer

programs banned from use. However, the examiner takes Official Notice that running separate processes on a computer is old and well established in the art of computer application processing as a method of increasing the modularity of software code. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to execute the anti computer virus logic as a separate instance. One of ordinary skill in the art would have been motivated to perform such a modification to allow the use of the software separately from other software components. This advantage is well known to those skilled in the art.

12. Claims 2-3, 8-9, 16-17, 22-23, 30-31, 36-37 are rejected under 35 U.S.C. 103(a) as being unpatentable over Symantec in view of Hedberg, as applied to claim 1 above, in further view of "Bad IDEA" by Peter Szor (Szor), in further view of "Cryptography in Everyday Life" by Sarah Simpson (Simpson). Symantec, as modified above, lacks encrypting the banned program identifying data with a private key. However, Szor teaches that to prevent modification of antivirus signature files, the files should be encrypted (page 19, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to encrypt the banned program identifying data. One of ordinary skill in the art would have been motivated to perform such a modification to prevent modification of antivirus signature files, as taught by Szor (page 19, ¶2). As modified, Symantec lacks using a PGP private key. However, Simpson teaches that by encrypting a file with a private key, the sender can be verified by decrypting it with the corresponding public key (page 1, ¶1) and that PGP provides such encryption and authentication (page 1, ¶2). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to use a PGP private key. One of ordinary skill in

the art would have been motivated to perform such a modification to verify the creator of the signature files, as taught by Simpson (page 1).

13. Claims 5, 19 & 33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Symantec, in view of Hedberg, as applied to claims 4, 18 & 32 above, in further view of "Heuristic Anti-Virus Technology" by Veldman. Symantec, as modified above, discloses detecting variants of known viruses, but lacks the banned program identifying data including heuristic data identifying one or more behavioral characteristics. However, Veldman teaches that using heuristics and examining behaviors of a program allows detection of unknown viruses (§1 & §2.1). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to including in the identifying data, heuristic data identifying one or more behavioral characteristics. One of ordinary skill in the art would have been motivated to perform such a modification to detect unknown computer viruses, as taught by Veldman (§1, ¶1 & §2.1).

14. Claims 10, 24 & 38 are rejected under 35 U.S.C. 103(a) as being unpatentable over Symantec, in view of Hedberg, Szor & Simpson, as applied to claims 8, 22 & 36, in further view of U.S. Patent 5,844,986 to Davis. Symantec, as modified above, lacks storing the identifying data in a secure memory region. However, Davis teaches that to prevent a virus from corrupting a BIOS (flash memory), an authentication and validation procedure is required before its contents can be modified (col. 1, lines 32-45 & 63-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to store the identifying data in a secure memory region (memory requiring authentication). One of ordinary skill in the

art would have been motivated to perform such a modification to prevent a virus from corrupting the identifying data, as taught by Davis (col. 1, lines 32-45 & 63-67).

Conclusion

15. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Michael J. Simitoski whose telephone number is (703)305-8191. The examiner can normally be reached on Monday - Thursday, 6:45 a.m. - 4:15 p.m.. The examiner can also be reached on alternate Fridays from 6:45 a.m. – 3:15 p.m.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gregory Morse can be reached on (703)308-4789.

Any response to this action should be mailed to:
Commissioner of Patents and Trademarks
Washington, DC 20231
Or faxed to:
(703)746-7239 (for formal communications intended for entry)
Or:
(703)746-7240 (for informal or draft communications, please label "PROPOSED" or "DRAFT")
Hand-delivered responses should be brought to Crystal Park II, 2121 Crystal Drive, Arlington, VA 22202, Fourth Floor (Receptionist).

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is (703) 305-9000.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR

system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

MJS
September 15, 2004

GREGORY MORSE
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100